# Release Notes for RFS 4010 v5.0.3.0-001R

1 Introduction ..... 1
2 Accessing a Wi-NG v5 System ..... 1
3 Access Points Supported ..... 3
4 Installation Guidelines ..... 4
4.1 Firmware Upgrade Procedure ..... 4
4.1.1 Upgrade the RFS 4010 Switch to 5.0.3.0-001R from a 5.0.0.0-XXXB( beta) or R ( released) image ..... 4
4.1.2 Upgrade the RFS 4010 Switch to a 5.0.3.0-001R from a v4.1.X.X-XXR image ..... 4
4.1.3 Downgrade the RFS 4010 Switch to a 4.1.X.X-XXXR from a v5.0.3.0-001R image ..... 4
4.2 Auto-Install Procedure ..... 5
5 Important Notes ..... 5

## 1 Introduction

Motorola Enterprise Networking & Communications is releasing a maintenance release, Wi-NG v5.0.3.0-001R. This release addresses a potential security risk when accessing an RFS 4010 running v5.0.0.0-107R via the GUI.

It is recommended that users currently on the v5.0.0.0-107R upgrade their systems to v5.0.3.0-001R at the earliest.

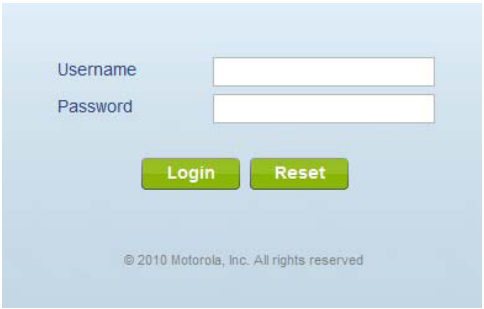
## 2 Accessing a Wi-NG v5 System

To access the RFS 4010 when running Wi-NG v5:

1. Connect one end of an Ethernet cable to any of the five LAN ports on the front of the RFS 4010 and connect the other end to a computer with a working web browser.

2. Set the computer to use an IP address between 192.168.0.10 and 192.168.0.250 on the connected port. Set a subnet / network mask of 255.255.255.0.

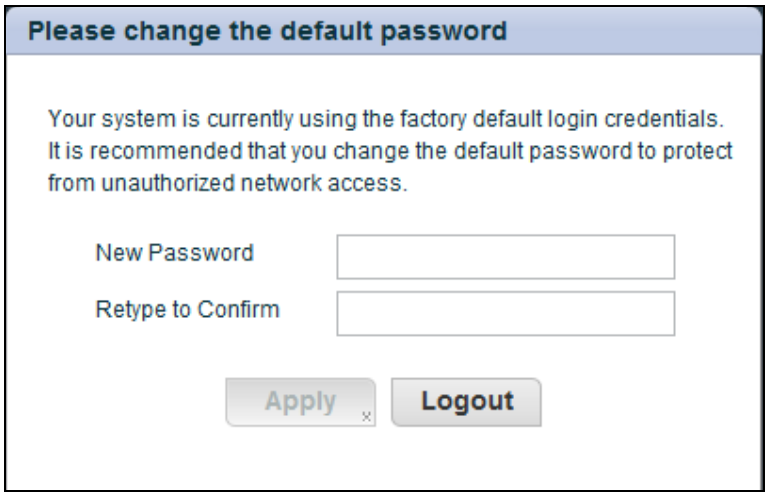
3. Once the computer has an IP address, point the web browser to: **http://192.168.0.1/** and the following Login screen will display.



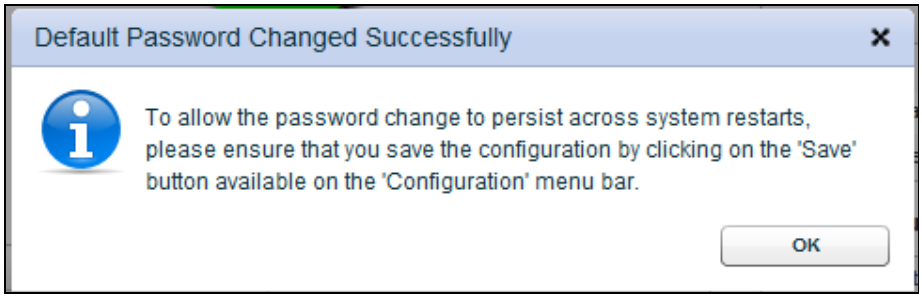

The login credentials for superuser access into a Wi-NG 5.0 system are :
**Username** : admin
**Password** : motorola

***When accessing the RFS 4010 system through the CLI,*** the same credentials as noted above for username and password will provide access i.e. admin/motorola. The user does not need to enter « cli » as the response to the first login prompt – that pertains only to a Wi-NG v4.x system.

The password must be changed after the initial login, as a security precaution, to prevent unauthorized access. You can re-enter the default but until the password is changed from the default the system will prompt for a new password with each login.


Please change the default password
Your system is currently using the factory default login credentials.
It is recommended that you change the default password to protect
from unauthorized network access.
New Password
Retype to Confirm
Apply
Logout

To make the password change permanent the configuration change will also need be saved.

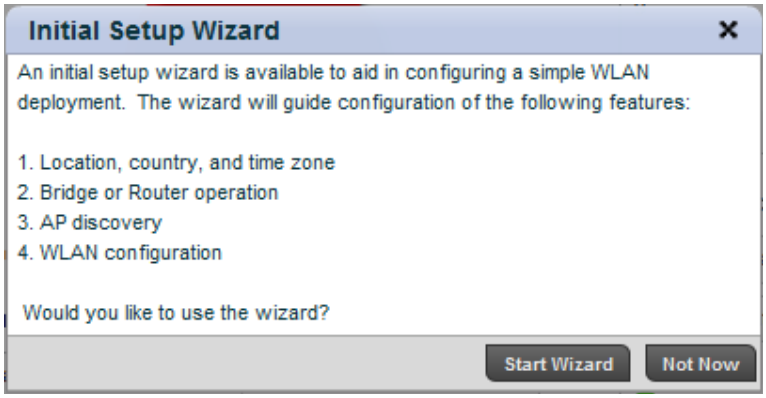

Default Password Changed Successfully
To allow the password change to persist across system restarts,
please ensure that you save the configuration by clicking on the 'Save'
button available on the 'Configuration' menu bar.
OK

Similar to a Wi-NG v4.x system, various user roles are supported to access the RFS 4010 controller.

| | |
|---|---|
| **Superuser** | Select this option to assign complete administrative rights to the user. This entails all the roles listed for all the other administrative roles. |
| **System** | Select System to allow the administrator to configure general settings like NTP, boot parameters, licenses, perform image upgrade, auto install, manager redundancy/clustering and control access. |
| **Network** | Select this option to allow the user to configure all wired and wireless parameters (IP configuration, VLANs, L2/L3 security, WLANs, radios etc). |
| **Security** | Select this option to allow the user to configure /edit WLAN keys |
| **Monitor** | Select Monitor to assign permissions without any administrative rights. The Monitor option provides read-only permissions. |
| **Help Desk** | Assign this role to someone who typically troubleshoots and debugs problems reported by the customer. The Help Desk manager typically runs troubleshooting utilities (like a sniffer), executes service commands, views/retrieves logs and reboots the controller. |

| | |
|---|---|
| **Web User** | Select Web User to assign the administrator privileges needed to add users for captive portal authentication. |

Upon initial login, the user will be presented with a “Quick-Start wizard”, that will help guide through the initial configurations for network set up.


Initial Setup Wizard
An initial setup wizard is available to aid in configuring a simple WLAN deployment. The wizard will guide configuration of the following features:
1. Location, country, and time zone
2. Bridge or Router operation
3. AP discovery
4. WLAN configuration
Would you like to use the wizard?
Start Wizard
Not Now

Similar to the Wi-NG v4.x system, the Wi-NG v5.0 solution also provides a dashbaord for the network, so that users can access the health of the system via key performance indicators, either at an RF Domain level, or at a granular device level. The Network View is a visual representation of a logical view of the network elements.

# 3 Access Points Supported

| Access Point | Firmware Version | Notes |
|---|---|---|
| AP 650 | 5.0.3.0-001R | This firmware version supports wireless access as well as Air Defense sensor capabilities – in simultaneous operation.<br><br>This firmware version on the AP 650 can be used to deploy it as a stand alone sensor, operating with Air Defense Services Platform v8.0.3 |

***Note***: Currently only the AP 650 802.11n Dependent Access Point is supported in Wi-NG v5.0. When adopted by an RFS 4010 running Wi-NG v5.0, the AP 650 dual radio 802.11n Dependent Access Point:

- can provide simultaneous access in 2.4GHz and 5 GHz
- can dedicate one radio to be a dual band sensor radio for the Air Defense solution OR the native security engine built-into the Wi-NG 5 OS, while the second radio can provide wireless access in either 2.4 or 5 GHz
- can locally bridge and forward traffic, without the packets having to go through the controller
- cannot survive without a controller.If there is loss of communication to the controller, and a redundant controllr in either active or standby mode is not available, the AP 650 will cease operation till connectivity to the controller is restored

**The AP 650 can be operated in the following modes:**

- 1X1
- 2X2
- 2X3
- 3X3

- Dynamic Chain Selection – this optimizes legacy client behavior

**In the Wi-NG 5.0 paradigm, each radio now supports 8 BSSIDs.**

| Product | BSSIDs supported | ESSIDs supported | Notes |
|---|---|---|---|
| AP 650 Dual Radio SKUs | 16 | 32 | 16 SSIDs are hidden |
| AP 650 Single Radio SKUs | 8 | 16 | 8 SSIDs are hidden |

# 4 Installation Guidelines

For accessing the Graphical User Interface (GUI) of the RFS 4010 services controller, a browser supporting Flash Player 10 is required( minimum version 10.0.32). The system accessing the GUI should have a minimum of 512Mb or RAM for the UI to function properly Wi-NG v5.0 is based on Flex, and does not use Java as the underlying UI framework. Java continues to be used in the Wi-NG v4.x framework. The following browsers have been validated

1. Firefox 3.x
2. IE 7.x/8.x
3. Google Chrome 6.x
4. Apple Safari 5.x

## 4.1 Firmware Upgrade Procedure

This section outlines the upgrade procedure to v5.0 from Released version from previous beta images on the RFS 4010.

The method described in this section uses the Command Line Interface (CLI) and GUI and the Auto-Install procedures. To log into the CLI, either SSH, Telnet or serial access can be used.

### 4.1.1 Upgrade the RFS 4010 Switch to 5.0.3.0-001R from a 5.0.0.0-XXXB( beta) or R ( released) image

1. Copy the RFS4000-5.0.3.0-001R.img to your tftp/ftp server.
2. Use the "**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**" , or "**upgrade tftp://<ip address of server>/<name of file>**" command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the switch. From CLI the command is "reload".

### 4.1.2 Upgrade the RFS 4010 Switch to a 5.0.3.0-001R from a v4.1.X.X-XXR image

1. Copy the RFS4000-5.0.3.0-001R.img to your tftp/ftp server.
2. Use the "**upgrade ftp://<ip address of server>/<name of file>**" command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the switch. From CLI the command is "reload".

***Note*:** When upgrading from Wi-NG v4.x to Wi-NG v5 system, the configuration is not retained or converted. All configuration will go back to a v5.0 factory defaults. Only IP connectivity information is maintained through the upgrade. The rest of the condifuration has to be rebuilt.

### 4.1.3 Downgrade the RFS 4010 Switch to a 4.1.X.X-XXXR from a v5.0.3.0-001R image

1. Copy the RFS4000-4.1.X.X-XXXR.img to your tftp/ftp server.
2. Use the "**upgrade ftp://<ip address of server>/<name of file>**" command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the switch. From CLI the command is "reload".

## 4.2 Auto-Install Procedure

Auto Install in v5.0.3 works via the DHCP server. This requires the definition of a Motorola Vendor Class and four sub-options that can be either sent seperately, or under option 43:

- Option 186 - defines the tftp/ftp server and ftp username, password information( IP address and protocol need to entered as a string: “ftp://admin:motorola@192.168.1.10”)
- Option 187 - defines the firmware path and file name
- Option 188 - defines the config path and file name
- Option 190 - defines the cluster config path and file name.

*Note that the DHCP vendor class for the RFS4000 is MotorolaRFS.RFS4000”.*

Autoinstall of firmware and autoinstall of configuration can be enabled or disabled.

# 5 Important Notes

1. Default configuration for the RFS4010 v5.0.3 ( same as 5.0) is detailed below:

   - VLAN1 has DHCP as primary IP address and the fixed address 192.168.0.1/24 as secondary
   - All ports are in VLAN1
   - The default bridging-policy disables local-bridging on access points
   - Stateful firewall is enabled with an implicit allow-all policy. Out-of-state packets will be dropped.
   - There is a wlan named wlan1 with ssid of "motorola". This wlan is disabled.
   - http, https and ssh are enabled in the default management-policy
   - Default users are admin/motorola and operator/operator.
   - APs that adopt will use the default management-policy (ssh is enabled)
   - SNMPv2 is disabled, community string is "public" and access is read-only
   - SNMPv3 is enabled, users are "snmpoperator/operator", "snmptrap/motorola" and "snmpmanager/motorola". Please note that SNMP is only available for MIB II traps currently. Configuration via SNMP GETS is not available.
   - DHCP options based "autoinstall" feature is enabled by default for configuration and firmware updates

2. There is also a "Gateway-startup-config" file which can be copied to startup-config. This has:

   - GE1-GE5 on VLAN 1 with static ip of 192.168.0.1
   - UP1 is mapped to VLAN 2100 with dhcp IP
   - DHCP server is enabled in vlan2 serving IP addresses in the range 192.168.0.100 to 192.168.0.254
   - L2 firewall is disabled.

3. Please see maximum capacities supported below:

| **Category** | **Capacity** |
|---|---|
| AP per controller | 6 |
| WLANs per controller | 24 |
| L3 VLANs per controller | 32 |
| ACLS | 500 |
| VPN tunnels | 256 |
| Firewall sessions | 50,000 |
| Number of RADIUS users for the onboard RADIUS | 500 |
| Wireless clients per AP | 256 associations |
| Wireless clients per RFS 4010 | 500 |
| Number of controllers in a cluster | 12 |